Listing of Claims:

Claim 1. (Currently Amended) A secure detection network system having a plurality of nodes, each node comprising a processor and storage means, the system comprising:

A. a plurality of remote nodes, each remote node comprising a set of detector interfaces configured to couple to a set of detectors disposed to detect the presence of an illegal asset within a shipping container;

B. at least one server node configured to initialize and install each remote node in the plurality of remote nodes, including delivering to each remote node an agent module, said agent module for each remote node comprising a node specific configuration file defining a set of nodes with which the remote node can communicate and a different encryption means corresponding to each node in the set of nodes; ~~and~~

C. a communication path coupling the plurality of remote nodes and the at least one server node; and

D. orthogonal authentication means for selectively restricting access to at least one of the plurality of remote nodes.

Claim 2. (Original) The system of claim 1 wherein the at least one server node includes a strobing module configured to selectively initiate coordinated strobing of the encryption means among the plurality of remote nodes.

Claim 3. (Original) The system of claim 1 wherein at least some of the plurality of remote nodes includes a wireless communication means, the communication path includes an air path.

Claim 4. (Original) The system of claim 1 wherein the at least one server node includes a wireless communication means, the communication path includes an air path.

Claim 5. (Original) The system of claim 1 wherein the at least one server node includes an audit module configured to selectively cause one or more of the remote nodes to terminate communication with at least one node in its set of nodes in response to one or more termination events.

Claim 6. (Original) The system of claim 5, wherein the one or more termination events includes detecting tampering with one or more remote nodes.

Claim 7. (Original) The system of claim 1, wherein the illegal assets includes one or more of chemical weapons, biological weapons or nuclear weapons.

Claim 8. (Original) The system of claim 1, wherein the illegal assets includes one or more of chemical agents, biological agents, radioactive materials, illegal drugs, or explosive materials or devices.

Claim 9. (Original) The system of claim 1, wherein one or more remote nodes from the plurality of remote nodes is disposed within a tamper resistant housing coupled to a shipping container.

Claim 10. (Original) The system of claim 1, comprising one or more subnetworks comprising a set of remote nodes from the plurality of remote nodes, and wherein each subnetwork provides a portion of the communication path.

Claim 11. (Currently Amended) The system of claim 1, further comprising:

~~D.~~E. a robot node, having a robot agent module and an interface to the communication path, the monitor node including means to query each of the plurality of remote nodes.

Claim 12. (Original) The system of claim 11, wherein the robot node is configured to query one of the plurality of remote nodes via a set of other remote nodes from the plurality of remote nodes.

Claim 13. (Currently Amended) The system of claim 1, further comprising:

~~D.~~E. a monitor node coupled to the communication path and configured to audit the plurality of remote notes.

Claim 14. (Original) The system of claim 13, wherein the at least one monitor node and the at least one server node are configured to communicate with at least one remote node from the plurality of remote nodes via one or more other intermediate remote nodes.

Claim 15. (Withdrawn) The system of claim 1, further comprising an orthogonal means of authentication.

Claim 16. (Original) A system of claim 1, wherein at least one remote node is housed within a tamper resistant package with at least one detector.

Claim 17. (Currently Amended) A secure detection node comprising:

A. a secure network interface, configured to receive an agent module and node-specific configuration files via a secure network;

B. a processor and a memory, the processor configured to execute the agent module, the agent module configured to implement the node-specific configuration files to establish a different encryption means for each node from a set of nodes with which the secure detection node is to communicate; ~~and~~

C. a detector interface, configured to receive data from a set of detectors disposed to detect the presence of an illegal condition; and

D. orthogonal authentication means for selectively restricting access to at least one of the plurality of remote nodes.

Claim 18. (Currently Amended) The node of claim 17, further comprising:

~~D.~~E. a tamper resistant box within which the processor and memory are housed.

Claim 19. (Currently Amended) The node of claim 17, further comprising:

~~D.~~E. at least one detector from the set of detectors.

Claim 20. (Currently Amended) The node of claim 19, further comprising:

~~D.~~F. a tamper resistant box within which the processor, memory and at least one detector are housed.

Claim 21. (Currently Amended) A method of providing a secure detection network system having a plurality of nodes, each node comprising a processor and storage means, the method comprising:

A. providing a plurality of remote nodes, each remote node comprising a set of detector interfaces configured for coupling to a set of detectors disposed for detecting the presence of an illegal condition within a shipping container;

B. generating by at least one server node an intelligent agent module and a set of node specific configuration files for each remote node in the plurality of remote nodes, including defining for each remote node a set of other nodes with which the remote node can communicate, including providing a different encryption means corresponding to each node in the set other nodes;

C. downloading to each remote node via a communication path a corresponding intelligent agent module and a corresponding set of node specific configuration files; ~~and~~

D. installing each remote node in the plurality of remote nodes, including executing the corresponding intelligent agent module with the corresponding node specific configuration files; and

E. selectively restricting access to at least one of the plurality of remote nodes by at least one orthogonal authentication.

Claim 22. (Currently Amended) The method of claim 21 further including strobing the encryption means among the plurality of remote nodes.

Claim 23. (Original) The method of claim 21 further including providing for at least some of the plurality of remote nodes a wireless communication means, the communication path including an air path.

Claim 24. (Original) The method of claim 21 further including providing a wireless communication means for at least one monitor node, the communication path including an air path.

Claim 25. (Original) The method of claim 21 including selectively causing one or more of the plurality of remote nodes to terminate communication with at least one node in response to one or more termination events.

Claim 26. (Original) The method of claim 25, wherein the one or more termination events includes detecting tampering with one or more remote nodes.

Claim 27. (Original) The method of claim 21, wherein the illegal condition includes the presence of one or more suspicious materials, including chemical weapons, biological weapons, nuclear weapons, chemical agents, biological agents, radioactive materials, illegal drugs, explosive materials or devices, or shielding means.

Claim 28. (Original) The method of claim 21, wherein the illegal condition includes a suspicious activity, including an attempt to defeat a remote node or detector.

Claim 29. (Original) The method of claim 21, including installing one or more remote nodes from the plurality of remote nodes within a tamper resistant housing coupled to a shipping container.

Claim 30. (Original) The method of claim 21, including forming one or more subnetworks comprising a set of remotes nodes from the plurality of remote nodes, and wherein each subnetwork provides a portion of the communication path.

Claim 31. (Currently Amended) The method of claim 21, further comprising:

~~E.~~F. monitoring the plurality of remote nodes with at least one monitor node, including querying each of the plurality of remote nodes via the communication path.

Claim 32. (Original) The method of claim 31, wherein the at least one monitor nodes is a portable robot node.

Claim 33. (Original) The method of claim 31, including communicating between at least one remote node from the plurality of remote nodes and the at least one monitor node or the at least one server node via one or more other intermediate remote nodes.

Claim 34. (Withdrawn) A secure identification control system comprising:

A. at least one body sensor configured to sense biometric information from a body;

B. a handheld node comprising an interface to the at least one body sensor and an interface to a secure network, wherein the handheld node is configured to record biometric information, including information indicating removal of the body sensor from the body;

C. the secure network including at least one server node configured to deliver to the handheld node an agent module, said agent module comprising a node specific configuration file defining a set of nodes with which the handheld node can communicate and a different encryption means corresponding to each node in the set of nodes;

D. a set of detectors configured to sense a handheld node location; and

E. an identification controller coupled to the secure network and configured to generate an identification indication as a function of the handheld node location and an authentication of the body from the handheld node, wherein such authentication is a function of an indication from the handheld device that the at least one body sensor had not been removed from the body.

Claim 35. (Withdrawn) The secure identification control system of claim 34, wherein the set of detectors includes one or more detectors configured for communicating via florescent lights or by retroreflective illumination.

Claim 36. (Withdrawn) The secure identification control system of claim 34, wherein the body is a passenger in a vehicle.

Claim 37. (Withdrawn) The secure identification control system of claim 34, wherein the identification controller is configured for granting access to a secure facility or area.

Claim 38. (Withdrawn) The secure identification control system of claim 34, wherein the identification controller is configured for providing the identification indication to a friendly fire prevention detection system.

Claim 39. (Withdrawn) An orthogonal authentication system, comprising:

A. a computer system having a user interface and access to a network;

B. a user authentication subsystem comprising user specific authentication data for a plurality of users, and configured to authenticate a user as a function of authentication information input at the computer system;

C. a biometric database, comprising user specific biometric data for a plurality of users;

D. a facility access control system having access to the network and the biometric database, and including at least one biometric sensor and an access controller configured to grant access to a facility as a function of biometric data received from the at least one biometric sensor corresponding to a set of user specific biometric data in the biometric database; and

E. a computer network access controller configured to grant the user access to the network as a function of an authentication of the user by the user authentication subsystem and an identification of the user from the facility access control system.

Claim 40. (Withdrawn) The orthogonal authentication system of claim 39, wherein the at least one biometric sensor includes a face scanner, palm scanner, retina scanner or fingerprint scanner.

Claim 41. (Withdrawn) A method of providing orthogonal authentication for access to a computer network, the method comprising the steps:

A. granting access to a facility having a computer system therein as a function of sensing biometric data of a user that corresponds with stored user specific biometric data;

B. entering user authentication data at the computer subsystem;

C. authenticating the user by one or more of:

1. comparing the entered user authentication data with stored user specific authentication data; or

2. confirming the identity of the user employee by visual inspection;

D. granting the user access to the computer network if the user was granted access to the facility in step A and authenticated in step C, else refusing access to the network by the user.

Claim 42. (New)The system of claim 1, w erein the orthogonal authentication means comprises a physical authentication.

Claim 43. (New) The system of claim 42, wherein the physical authentication means is selected from the group consisting of: biometrics, physical facilities, human audit, telephones, hand geometry scanner, fingerprint scanner, facial scanner, and voice print scanner.